

AMENDMENTS TO THE SPECIFICATION

Pages 28-29

Please replace the paragraph commencing at line 15 of page 28 with the following amended paragraph:

At the time of T0, the key K₁ is supplied, and the encrypting process of the plaintext data M₁ is started. When the encrypting process of the plaintext data M₁ is started at the time of T0, the input of the selector 54 is switched to B after the initial value ~~IT-IV~~IV is once input from the input A of the selector 54. Further, at the time of X during the plaintext data M₁ is being encrypted using the key K₁, it is assumed an interrupt IT for requesting to encrypt the plaintext block data N₁ is generated. The ciphertext block data C₁ becomes to be stored in the memory 55 by the time of T1. Then, at the time of T1, the key K₂ is supplied to the encrypting module 51 due to the generation of the interrupt IT. Further, the selector 54 sets the input to A at the time of T1. The switch 57 is connected to F at the time of T1. After the time of T1, the plaintext block data N₁ is encrypted using the key K₂, and the ciphertext block data D₁ is output. At the time of Y, it is assumed the encryption of the plaintext block data N₁ is finished, and the interrupt IT is resolved. Due to the resolution of the interrupt IT, at the time of T2, the key K₁ is supplied to the encrypting module 51, the input of the selector 54 is switched to C, and the switch 57 is connected to E. By switching the selector 54 to C, the ciphertext block data C₁ stored in the memory 55 is input for encrypting the plaintext block data M₂, the plaintext block data M₂ is encrypted by the encrypting module using the key K₁, and the ciphertext block data C₂ is output. Before the time of T3, the input of the selector 54 is switched to B. In case of encrypting the plaintext block data M₃, the ciphertext block data C₂ is fed back from a feedback line 65 of a feedback loop and input, the plaintext block data M₃ is encrypted by the encrypting module using the key K₁, and the ciphertext block data C₃ is output.